The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
01/24/2017

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in iOS, tvOS, watchOS, macOS Sierra, iCloud for Windows, Safari, and iTunes for Windows, which could allow for arbitrary code execution. iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch. tvOS is an operating system for the fourth-generation Apple TV digital media player. watchOS is the mobile operating system of the Apple Watch and is based on the iOS operating system. macOS Sierra is the thirteenth major release of macOS (previously OS X), Apple's desktop and server operating system for Macintosh computers. iCloud for Windows is a service developed by Apple that keeps Apple devices in sync with each other. Safari is a web browser developed by Apple. iTunes for Windows is a media player, media library, online radio broadcaster, and mobile device management application developed by Apple.

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- iOS Versions prior to 10.2.1
- tvOS Versions prior to 10.1.1
- watchOS Versions prior to 3.1.3
- macOS Sierra Versions prior to 10.12.3
- iCloud for Windows Versions prior to 6.1.1
- Safari Versions prior to 10.0.3
- iTunes for Windows Versions prior to 12.5.5

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in watchOS, iOS, tvOS, macOS Sierra, iCloud for Windows, Safari, and iTunes for Windows. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- An arbitrary code execution vulnerability that affects a feature called 'FontParser' when processing a maliciously crafted font file. (CVE-2016-4691)
- An arbitrary code execution vulnerability caused by opening a maliciously crafted file due to an input validation issue existing in modelines. (CVE-2016-1248)
- An arbitrary code execution vulnerability that affects a feature called 'FontParser' when processing a maliciously crafted font file. (CVE-2016-4688)
- A security vulnerability which may allow an attacker to exploit weaknesses in the 3DES cryptographic algorithm. (CVE-2016-4693)
- An arbitrary code execution vulnerability that affects the 'CoreMedia Playback' module when processing a maliciously crafted .mp4 file. (CVE-2016-7588)
- An arbitrary code execution vulnerability caused by processing maliciously crafted web content. (CVE-2016-7589)
- An arbitrary code execution with kernel privileges vulnerability that affects a feature called 'IOHIDFamily'. (CVE-2016-7591)
- An arbitrary code execution vulnerability that affects a feature called 'ICU' when processing maliciously crafted web content. (CVE-2016-7594)
- An arbitrary code execution vulnerability that affects the 'CoreText' module when processing a maliciously crafted font file. (CVE-2016-7595)
- An insufficient initialization vulnerability allowing an application to read kernel memory was addressed by properly initializing memory returned to user space. (CVE-2016-7607)
- Multiple memory corruption vulnerabilities allowing an application to execute arbitrary code with kernel privileges were addressed through improved input validation. (CVE-2016-7606, CVE-2016-7612)
- A denial of service vulnerability allowing local user to cause a system denial of service was addressed through improved memory handling. (CVE-2016-7615)
- An arbitrary code execution with kernel privileges vulnerability that affects a feature called 'Disk Images' due to input validation errors. (CVE-2016-7616)
- A 'symlink' validation vulnerability allowing a local attacker to overwrite existing files. (CVE-2016-7619)
- An arbitrary code execution vulnerability allowing a local user to cause an unexpected system termination or arbitrary code execution in the kernel was addressed through improved memory management. (CVE-2016-7621)
- A denial of service vulnerability that affects the 'CoreGraphics' module when processing a maliciously crafted font file. (CVE-2016-7627)
- A denial of service vulnerability that affects the handling of OCSP responder URLs. (CVE-2016-7636)
- A memory corruption vulnerability allowing a user to gain root privileges was addressed through improved input validation. (CVE-2016-7637)

- A security vulnerability that affects a feature called ‘ImageIO’ which may allow for a remote attacker to leak memory. (CVE-2016-7643)
- An arbitrary code execution vulnerability may allow a local application with system privileges the ability to execute arbitrary code with kernel privileges. (CVE-2016-7644)
- An issue existed which did not reset the authorization settings on app uninstall. This issue was addressed through improved sanitization. (CVE-2016-7651).
- A memory corruption vulnerability which may allow an application to read kernel memory was addressed through improved input validation. (CVE-2016-7657)
- Memory corruption issues caused by processing maliciously crafted files leading to arbitrary code execution was addressed through improved input validation. (CVE-2016-7658, CVE-2016-7659)
- A privilege escalation vulnerability in mach port name references which may allow a local user to gain root privileges. (CVE-2016-7660)
- A memory-corruption vulnerability in the ‘CoreFoundation’ module when processing strings may lead to an unexpected application termination or arbitrary code execution. (CVE-2016-7663)
- Multiple issues in PHP were addressed by updating to PHP version 5.6.28. (CVE-2016-8670, CVE-2016-9933, CVE-2016-9934)
- An arbitrary code execution vulnerability exists when unpacking a maliciously crafted archive was addressed through improved memory handling. (CVE-2016-8687)
- A data exfiltration vulnerability exists in a prototype access issue by processing maliciously crafted web content was addressed through improved exception handling. (CVE-2017-2350)
- A security-bypass vulnerability with handling user input that causes a device to present the home screen even when locked. (CVE-2017-2351)
- A logic issue which may unlock an Apple Watch when it is off the user's wrist was addressed through improved state management. (CVE-2017-2352)
- An arbitrary code execution vulnerability exists in the Bluetooth feature was addressed through improved memory management. (CVE-2017-2353)
- An arbitrary code execution vulnerability caused by a memory initialization issue exists when processing maliciously crafted web content. (CVE-2017-2355)
- A security vulnerability may allow an application to determine kernel memory layout due to an uninitialized memory issue. (CVE-2017-2357)
- An arbitrary code execution with kernel privileges vulnerability caused by a memory corruption issue was addressed through improved input validation. (CVE-2017-2358)
- A state management vulnerability in the address bar caused by visiting a malicious website was addressed through improved URL handling. (CVE-2017-2359)
- An arbitrary code execution vulnerability may allow an application to execute arbitrary code with kernel privileges. (CVE-2017-2360)
- A data exfiltration vulnerability caused by a validation issue when processing maliciously crafted web content. (CVE-2017-2365)
- A denial of service vulnerability when processing a maliciously crafted contact card may lead to unexpected application termination. (CVE-2017-2368)
- An arbitrary code execution with kernel privileges vulnerability due to a buffer overflow issue was addressed through improved memory handling. (CVE-2017-2370)
- An arbitrary code execution vulnerability exists when processing maliciously crafted web content. (CVE-2017-2354, CVE-2017-2362, CVE-2017-2373)
- Multiple arbitrary code execution vulnerabilities caused by multiple memory corruption issues exist when processing maliciously crafted web content. (CVE-2017-2356, CVE-2017-2369, CVE-2017-2366)

- Multiple data exfiltration vulnerabilities are caused by processing maliciously crafted web content due to a validation issue existing in the handling of page loading. (CVE-2017-2363, CVE-2017-2364)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:
Apple:
https://support.apple.com/en-us/HT201222
https://support.apple.com/en-us/HT207486
https://support.apple.com/en-us/HT207484
https://support.apple.com/en-us/HT207481
https://support.apple.com/en-us/HT207483
https://support.apple.com/en-us/HT207482
https://support.apple.com/en-us/HT207485
https://support.apple.com/en-us/HT207487

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1248
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4688
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4691
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4693
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7588
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7589
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7591
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7594
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7595
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7606
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7607
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7612
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7615
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7616
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7619
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7621

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7626
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7627
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7636
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7637
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7643
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7644
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7651
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7657
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7658
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7659
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7660
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7662
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7663
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8670
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8687
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9933
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9934
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2350
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2351
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2352
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2353
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2354
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2355
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2356
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2357
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2358
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2359
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2360
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2361
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2362
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2363
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2364
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2365
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2366
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2368
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2369
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2370
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2371
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2373